به نام خدا

پروفایل حفاظتی سیستم جلوگیری از نفوذ

تیرماه ۹۶

نسخه ۲,۱۱

فهرست

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد. مرکز مدیریت راهبردی افتا با همکاری سازمان فناوری اطلاعات ایران این سند را در راستای این هدف تهیه کرده است. در این سند الرامات امنیتی IPS[۱] بیان می‌شود. البته این بسته‌ی تکمیلی به خودی خود کامل نیست، بلکه الحاقی بر الزامات امنیتی «پروفایل حفاظتی تجهیزات شبکه[۲]» یا «پروفایل حفاظتی دیواره آتش حالتمند» است. این بسته‌ی تکمیلی را باید همراه با پروفایل حفاظتی تجهیزات شبکه و/یا دیواره آتش حالتمند مورد استفاده قرار داد.

این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 تهیه گردیده است. همچنین فرهنگ اصطلاحات بکار رفته در این سند در پیوست شماره یک آمده است.

۲ شرح محصول جلوگیری از نفوذ

این بسته‌ی تکمیلی، به سیستم‌های جلوگیری از نفوذ (IPS) مبتنی بر شبکه می‌پردازد. IPS، محصولی است که به یک یا چند شبکه معین متصل شده و به عنوان بخشی از راه‌حل کلان امنیتی سازمان، مدیریت می‌شود. به طور خاص یک IPS، سرپرست امنیت شبکه را قادر به نظارت، جمع‌آوری، گزارش‌گیری و واکنش بلادرنگ به ترافیک مخرب در شبکه می‌سازد. تمرکز این بسته تکمیلی بر بازرسی ترافیک IP (TCP، UDP، ICMP و غیره) معطوف است. این محدودیت حوزه، بنا به دلایل زیر عمداً انتخاب شده است: تعیین یک مرز مناسب برای حوزه آزمون و ارزیابی (اقدامات تضمینی) که در این بسته تکمیلی تعیین شده است و اجازه دادن به بسته‌های تکمیلی آتی به منظور بررسی IPS ها و کارکردهای دیگری مثل اسکنرها[۳]، آنالیزورها[۴]، سنسورها[۵] و غیره. حوزه‌ی این

[۱] Intrusion Prevent System (IPS)
[۲] Security Requirements for Network Devices (NDPP)
[۳] Scanners
[۴] Analyzers
[۵] Sensors

بسته تکمیلی، مانع از ارزیابی پروتکل‌های IP دیگر مثل GRE، ESP، AH نیست، اما شامل ارزیابی پروتکل‌های غیر IP[۱] مانند پروتکل‌های لایه ۲ یا اترنت نیز نمی‌گردد.

الزامات اصلی این بسته تکمیلی، الزاماتی هستند که برای یک محصول جلوگیری از نفوذ، ضروری شناخته شده‌اند. با این حال، اهداف ارزیابی ممکن است کارکرد IPS را کاملاً مستقل از دیگر اجزای شبکه فراهم کنند و/یا طوری استقرار یابند که در ارتباط با اجزای دیگر در یک راه‌حل امنیت سازمانی بزرگ‌تر کار کنند. برای مثال، گرچه تمامی IPS های مورد ارزیابی باید ظرفیت‌هایی برای نظارت، جمع‌آوری، تجزیه و تحلیل و واکنش به ترافیک شبکه داشته باشند، اهداف ارزیابی مطابق این پروفایل می‌توانند:

- بر روی ترافیک‌هایی که از یک یا چند واسط می‌گذرد به صورت غیرفعال نظارت کند و/یا تنها جریان ترافیک خاصی را که از IPS می‌گذرد، مورد نظارت قرار دهد.
- داده‌های IPS را به یک میزبان ذخیره‌ساز ممیزی خارجی منتقل کند و در صورت انتخاب، داده‌های IPS را به صورت داخلی ذخیره نماید. داده‌های ممیزی IPS می‌توانند (توسط محصول) ارسال شوند یا (توسط میزبان راه دور) دریافت شوند. بدون توجه به اینکه داده‌های IPS دریافت یا ارسال می‌شوند، روند انتقال باید به روشی مورد حفاظت قرار گیرد که با الزامات ارتباطات حفاظت‌شده در بخش «محل ذخیره‌سازی داده‌های ممیزی» از «پروفایل حفاظتی تجهیزات شبکه» هماهنگ باشد.
- ترافیک شبکه را بر اساس تنظیماتی که سرپرست شبکه می‌تواند مستقیماً روی محصول پیاده کند، تجزیه و تحلیل نماید و در صورت انتخاب تحلیل ترافیک شبکه را بر اساس تنظیماتی که از سیستمی دیگر وارد شده است، فراهم نماید.
- به طور مستقل به ترافیک مخرب واکنش نشان دهد (مثل متوقف کردن جریان ترافیک، یا انتقال بسته توقف نشست به نقاط پایانی) و در صورت انتخاب، این کار را در همکاری با اجزای غیر محصول در راه‌حل کلان امنیتی سازمان، با ایجاد یک ارتباط به اجزای غیر محصول، انجام دهد تا باعث شود اجزای غیر محصول بتوانند مانع جریان ترافیک شوند.

شباهت‌های زیادی بین یک محصول IPS و یک سیستم کشف نفوذ (IDS) وجود دارد؛ اما تمایزات مهمی نیز وجود دارند. تفاوت IPS با IDS از این لحاظ است که IPS باید واکنش فعالی در جهت قطع کردن/ متوقف کردن یک تهدید فعال داشته باشد و بتواند به صورت بلادرنگ واکنشی در جهت قطع نمودن جریان ترافیک مشکوک داشته باشد. برای IPS تولید هشدار یا رویداد ممیزی در هنگام شناسایی یک ترافیک مخرب کافی نیست. البته،

[۱] Non-IP protocol

سرپرست IPS ممکن است محصول را طوری پیکربندی نماید که پاسخ‌های پیشگیرانه فعال نباشد و چنین پیکربندی برای محصول، پیکربندی معتبری خواهد بود. هرچند می‌توان تنها کارکردهای IDS را در محصول منطبق بر این پروفایل فعال نمود، اما چنین IPS باید قابلیت‌هایش را حین ارزیابی، نشان دهد.

اهداف ارزیابی با به‌کارگیری رویکردهای متنوع، ترافیک خرابکار شبکه را شناسایی می‌کنند. به بیان کلی‌تر، تجزیه و تحلیل شبکه می‌تواند مبتنی بر شناسایی تهدیدات «شناخته‌شده» یا «ناشناخته» باشد. شناسایی تهدیدات «شناخته‌شده» ممکن است از طریق تطبیق‌دهی الگوی تهدیدات صورت گیرد؛ مثلاً با تطبیق دهی رشته‌های کاراکتر درون یک بسته IP، یا با تطبیق دهی الگوی ترافیکی رایج در حملات DoS یا حملات اکتشاف و شناسایی[1]. شناسایی تهدیدات «ناشناخته» می‌تواند با استفاده از روش‌های متنوع شناسایی رفتارهای «غیرعادی» صورت گیرد. در این شیوه، الگوی ترافیک «مرسوم/ مورد انتظار» در اختیار IPS قرار می‌گیرد (یا آن را یاد می‌گیرد/ ایجاد می‌کند) تا بتواند الگوی ترافیکی «غیرعادی» را شناسایی کرده و به آن واکنش نشان دهد.

نویسندگان سند هدف امنیتی باید مناسب بودن پروفایل حفاظتی «فایروال» برای IPS مورد ارزیابی، علاوه بر پروفایل حفاظتی «تجهیزات شبکه» و «جلوگیری از تشخیص نفوذ» بررسی نمایند. در برخی موارد، بسته تکمیلی IPS ممکن است با محصول که برای تبعیت از بسته تکمیلی پروفایل حفاظتی فایروال پیکربندی شده است، سازگار نباشد، زیرا بسته تکمیلی «فایروال» ملزم می‌نماید که تمامی واسط‌ها انواع خاصی از ترافیک را تحت هر شرایطی بلوکه نمایند، درحالی‌که ممکن است برای تمامی اهداف ارزیابی IPS مناسب نباشد. با این حال، اگر نویسنده سند هدف امنیتی تمایل دارد که تمام پیکربندی‌های معتبر در محصول از تمامی الزامات کارکرد امنیتی در این بسته تکمیلی و در بسته تکمیلی «فایروال» پیروی کنند، تدوین‌کنندگان این بسته تکمیلی هیچ قصدی برای ایجاد عدم سازگاری بین این دو بسته تکمیلی ندارند.

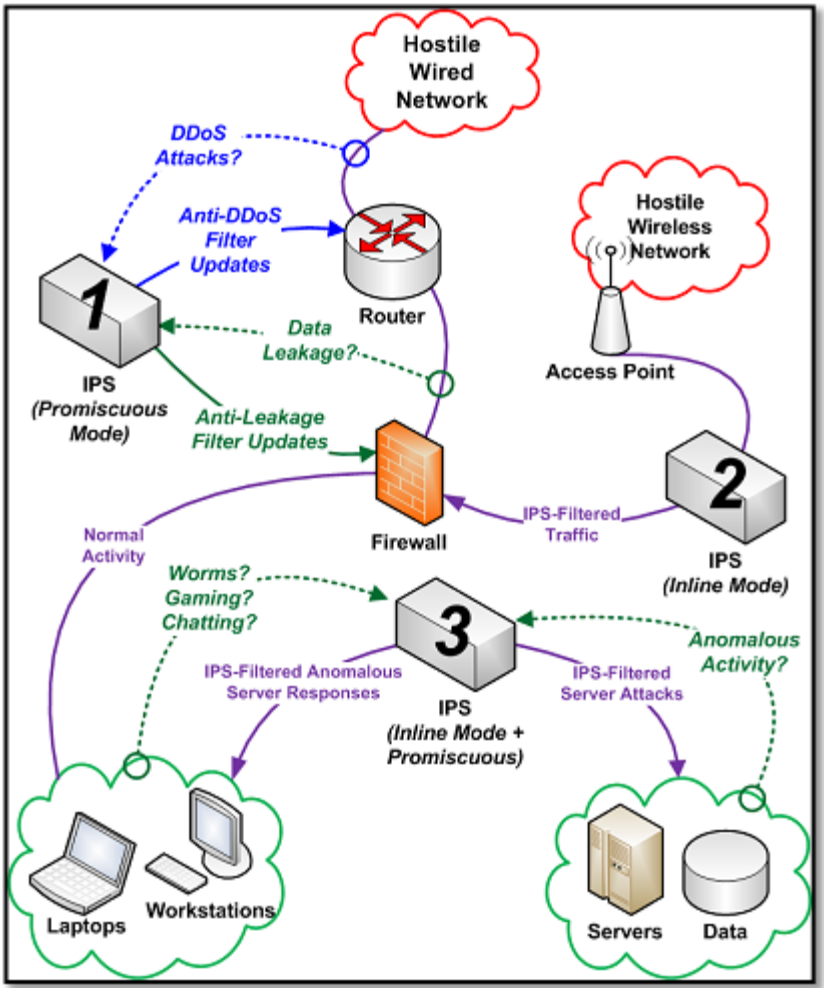
محصول ممکن است یک محصول توزیع‌شده باشد که برخی از الزامات کارکرد امنیتی یا عناصر این الزامات، توسط بخش‌های مجزای محصول اجرا شوند؛ بخش‌های مجزایی که در سراسر شبکه IP توزیع شده‌اند. در چنین مواردی، مرز محصول باید طوری مشخص شود که جمع کلی همه‌ی مؤلفه‌های محصول بتواند الزامات ذکر شده در این سند را برآورده سازد و هر مؤلفه خصوصی قادر به برآورده ساختن پروفایل حفاظتی تجهیزات شبکه یا دیواره آتش حالتمند درون خود باشد. به‌علاوه، تمامی روابط بین این مؤلفه‌های توزیع شده باید با استفاده از یک یا چند پروتکل مورد اعتماد ذکر شده در پروفایل حفاظتی تجهیزات شبکه یا دیواره آتش حالتمند، محافظت شوند.

[1] Reconnaissance

روش‌های استقرار که توسط محصول پشتیبانی می‌شوند، در شکل ۱ نشان داده شده‌اند. این روش‌ها شامل چند روش استقرار کارکرد IPS درون یک شبکه واحد نیز می‌شود.

- **IPS 1** در حالت بی‌قاعده[1] عمل می‌کند و داده‌ها را از دو شبکه مجزا خارج از حیطه فایروال دریافت می‌کند و نسخه‌های به‌روزرسانی فیلتر ترافیک را بر حسب نیاز به مسیریاب و فایروال پیرامونی ارسال می‌کند تا به صورت بلادرنگ، ترافیک ناخواسته را متوقف کنند.
- **IPS 2** در حالت درون‌خطی[2] عمل می‌کند و ترافیک دریافتی و ارسالی به یک شبکه وایرلس را تحلیل می‌نماید و به صورت بلادرنگ، هرگونه ترافیکی که خط‌مشی‌های IPS را طبق تعریف سرپرست سیستم نقض کند، متوقف می‌نماید.
- **IPS 3** در ترکیبی از حالت‌های بی‌قاعده و درون‌خطی عمل می‌کند. IPS حداقل یک جفت واسط دارد که پل یا مسیری را به محصول ایجاد می‌کنند و ترافیک را به صورت بلادرنگ حین عبور از محصول مورد تجزیه و تحلیل و فیلترینگ قرار می‌دهد. IPS مشابه، یک یا چند واسط بی‌قاعده دارد که ترافیک عبوری از هر شبکه مجزا را جمع‌آوری و تحلیل می‌کنند و به فعالیت‌های غیرعادی، کرم‌ها، یا دیگر فعالیت‌های تأیید نشده، واکنش نشان می‌دهند.

[1] Promiscuous
[2] Inline



شکل ۱: سناریو توسعه محصول

۳ مسائل امنیتی

دستگاه‌های IPS بازه‌ای از تهدیدات امنیتی مرتبط با تشخیص و واکنش به ترافیک بدخواه بر روی شبکه‌های نظارت شده را، جهت اجرایی شدن خط‌مشی‌های امنیتی بر روی ترافیک شبکه قابل‌اجرا، مقابله می‌کنند. ترافیک بدخواه ممکن است یک تهدید را به یکی یا تعداد بیشتری از نقاط پایانی شبکه نظارت شده، یا به زیرساختار شبکه، یا به خود IPS مورد طرح قرار دهد. اصطلاح شبکه نظارت شده در اینجا برای بیان هر شبکه‌ای که محصول، سگمنت/زیرشبکه‌های از شبکه که ترافیک خود را برای تحلیل و بررسی به سیستم تشخصی نفوذ فرستاده‌اند یا تغییر مسیر[۱] داده‌اند، مستقیماً به آن متصل است به کار می‌رود.

اصطلاح داده سیستم تشخیص نفوذ که در این سند مورد استفاده قرار گرفته است، هر داده یا همه داده‌ای را که از ترافیک شبکه استخراج شده است و بر روی هدف ارزیابی ذخیره شده است، نتیجه‌های تحلیل و بررسی انجام شده توسط هدف ارزیابی و پیام‌های که واکنش هدف ارزیابی را نسبت به تحلیل و بررسی نشان می‌دهد را شامل

[۱] Redirect

می‌شود. داده سیستم تشخیص نفوذ در این سند به داده جمع‌آوری شده توسط سیستم تشخیص نفوذ و نتیجه رکوردهای ممیزی مرتبط با تحلیل و بررسی ترافیک شبکه، اشاره دارد؛ و داده سیستم تشخیص نفوذ مجزا از داده ممیزی بیان شده در الزام «تولید داده ممیزی ۱» مربوط به پروفایل حفاظتی، مانند رکوردهای ممیزی مرتبط با احراز هویت مدیران و برقراری/خاتمه کانال‌های مورد اطمینان، است.

یک سایت مسئول توسعه خط‌مشی امنیتی خودش و پیکره‌بندی یک مجموعه نقش است که سیستم‌های تشخیص نفوذ اجرا خواهند کرد و یک پاسخ مناسب برای مواجهه با نیازهایشان، در رابطه با ریسک تحلیل و بررسی و تهدیدات دریافت شده توسط آن‌ها، تهیه خواهد کرد. تهدیدات رفع شده[۱] به‌وسیله یک هدف ارزیابی می‌تواند شامل تلاش‌های برای:

- اجرای اکتشاف[۲] مبتنی بر شبکه (کاوش برای اطلاعات در مورد شبکه نظارت شده و نقاط پایانی آن)، برای مثال، از طریق استفاده از تکنیک‌های متنوع پویش و نگاشت.
- مسدود کردن کارکرد طبیعی شبکه نظارت شده، نقاط پایانی، یا سرویس‌ها برای مثال، از طریق حملات محرومیت از سرویس[۳].
- به دست آوردن دسترسی نامناسب به یک یا تعداد بیشتری شبکه، نقاط پایانی، یا سرویس‌ها، برای مثال، از طریق حملات جستجوی فراگیر[۴] حدس رمز عبور، یا به‌وسیله مخابره کد، اسکریپت یا دستورات قابل اجرا.
- فاش‌سازی/مخابره اطلاعات با تخطی از خط‌مشی‌ها، برای مثال، فرستادن شماره کارت‌های اعتباری. در ارتباط با این داده‌ها مکان قرارگیری عامل تهدید مهم نیست. مثال، خروج داده[۵] به این معنی است که داده بدون داشتن مجوزی جهت حذف آن، حذف شده است؛ که ممکن است از طریق یک نفوذ از بیرون یا نتیجه یک اقدام رد داخل باشد.

توجه شود که این سند تهدیدات شناسایی شده در پروفایل حفاظتی تجهیزات شبکه یا پروفایل حفاظتی دیواره آتش حالتمند را تکرار نمی‌کند، اگرچه همه آن‌ها انطباق[۶] داده شده و بنابراین وابستگی این سند به پروفایل حفاظتی تجهیزات شبکه یا پروفایل حفاظتی دیواره آتش حالتمند را اعمال می‌کنند. به علاوه، این سند کارآمدی هدف ارزیابی (مانند توابع مدیریت امنیت) که با آنچه در پروفایل حفاظتی تجهیزات شبکه و پروفایل حفاظتی دیواره آتش حالتمند شناسایی شده، در معرض تهدیدات یکسانی است را تشریح می‌کند.

---

۱ Mitigated
۲ Reconnaissance
۳ Denial of service
۴ Brute force
۵ Data exfiltration
۶ Conformance

در واقع پروفایل حفاظتی تجهیزات شبکه تنها حاوی تهدیداتی برای توانایی هدف ارزیابی جهت تهیه توابع خودش، است. پروفایل حفاظتی دیواره آتش همه تهدیدات موجود در پروفایل حفاظتی تجهیز شبکه را به علاوه تهدیدات مربوط به منابع محیط عملیات هدف ارزیابی را شامل می‌شود. این سند بر روی تهدیدات مربوط به محیط عملیاتی نیز تمرکز دارد، بعضی از آن‌ها با تهدیدات تعریف شده در پروفایل حفاظتی دیواره آتش یکسان است ولی از منظر سیستم‌های تشخیص نفوذ به جای فیلتر ترافیک، ملاقات خواهند شد. در نتیجه تهدیدات مطرح شده در یک پروفایل حفاظتی پایه و تهدیدات مطرح شده در این سند باهم یک مجموعه جامع از تهدیدات امنیتی که به‌وسیله یک سیستم تشخیص نفوذ هدف ارزیابی، آدرسی دهی شده است را فراهم می‌سازند.

۳,۱ فاش‌سازی غیرمجاز اطلاعات

اطلاعات حساس روی یک شبکه محافظت شده ممکن است در نتیجه فاش‌سازی/مخابره اطلاعات با تخطی از خط‌مشی، مانند فرستادن شماره کارت‌های اعتباری به صورت رمز نشده، افشا شوند. سیستم تشخیص نفوذ هدف ارزیابی قادر خواهد بود محموله‌های بسته را برای الگوها و رشته‌های داده‌ای کاراکترها مورد تفتیش قرار دهد.

۳,۲ دسترسی غیرمجاز

یک مهاجم ممکن تلاش کند تا با استفاده از یک حمله جستجوی فراگیر، یا به‌وسیله مخابره کد، اسکریپت یا دستورات قابل اجرا، به یک یا تعداد بیشتری از شبکه‌ها، نقاط پایانی، یا سرویس‌ها، دسترسی غیرمجاز پیدا کند. اگر دستگاه‌های خارجی بدخواه قادر به ارتباط با دستگاه‌های موجود بر روی شبکه محافظت شده باشند، آنگاه آن دستگاه‌ها مستعد افشای غیرمجاز اطلاعات خواهند بود.

۳,۳ دسترسی نامناسب به سرویس‌ها

شبکه محافظت شده ممکن است خلاف خط‌مشی‌های محیط عملیاتی استفاده شده باشد که دسترسی به سرویس‌ها قابل دسترس می‌شود. دستگاه‌هایی که بیرون از شبکه محافظت شده قرار دارند ممکن است هنگام ارتباط با سرویس‌هایی که به‌صورت عمومی اجازه استفاده از آن‌ها وجود دارد، اقدام به تولید فعالیت‌های نامناسب کنند (برای نمونه، دست‌کاری ابزارهای موجود، تزریق SQL، راه‌اندازی مجدد اجباری، بارگذاری فایل‌های بدخواه، بات‌نت و ابزارهای دور زدن مجوزها).

۳,۴ قطع یا محرومیت از سرویس

حملات روی سرویس‌های داخل یک شبکه محافظت شده، یا به‌صورت غیرمستقیم با پرهیز از دسترسی دادن به عامل‌های بدخواه در داخل شبکه محافظت شده، ممکن است موجب محرومیت از سرویس در داخل شبکه محافظت شده شود. اتمام منبع ممکن است در رویداد، جریان درخواست هماهنگی سرویس از سوی تعداد کمی منابع، اتفاق بیافتد. اگرچه اکثر سیستم‌های تشخیص نفوذ برخی محافظت‌ها علیه حملات محرومیت از سرویس

توزیع شده، انجام می‌دهند ولی تهیه حفاظت برای محرومیت از سرویس توزیع‌شده یک الزام برای انطباق هدف ارزیابی نیست. توجه شود که به هرحال حفاظت از حمله محرومیت از سرویس الزامی است.

۳,۵ اهداف امنیتی

مشکلات امنیتی مطرح شده در قسمت قبل، به‌وسیله ترکیب توانایی‌های IPS به همراه فهم اینکه نصب محصول به گونه ایست که خط‌مشی‌هایش به‌صورت مؤثری بر روی ترافیک مربوط به شبکه‌های تحت نظارت قابل اجراست، پوشش داده می‌شود. انطباق محصول قابلیت امنیتی را فراهم خواهد ساخت که قادر به پوشش تهدیدات محصول، امکان اعمال فرآیندهای تحلیلی روی داده‌های جمع‌آوری شده ترافیک شبکه و اجرای خط‌مشی‌های شرکتی برای IPS ها به‌وسیله مدیران IPS، است. در ادامه اهداف امنیتی مرتبط با تهدیدات/خط‌مشی‌های ذکر شده، آورده شده است. قابل ذکر است که در کنار هر هدف امنیتی، مواردی از الزامات کارکرد امنیتی که برای آن هدف امنیتی لازم می‌باشند، آورده شده است.

۳,۵,۱ پایش سیستم

برای اینکه توانایی تحلیل و واکنش نسبت به تخطی‌ها از خط‌مشی‌های بالقوه شبکه، وجود داشته باشد، IPS باید قادر به جمع‌آوری و ذخیره المان‌های داده‌ای ضروری ترافیک شبکه مربوط به شبکه‌های تحت نظارت باشد.

۳,۵,۲ **تحلیل** تخطی‌ها از خط‌مشی ترافیک شبکه

موجودیت‌هایی که روی شبکه تحت نظارت قرار دارند یا ارتباط برقرار می‌کنند، باید تحلیل مؤثر فعالیت شبکه برای تخطی‌های بالقوه مربوط استفاده از شبکه را داشته باشند. محصول باید امکان تحلیل مؤثر داده جمع‌آوری شده از شبکه‌های تحت نظارت را برای کاهش ریسک مربوط به افشای غیرمجاز اطلاعات، دسترسی نادرست به سرویس‌ها و سوءاستفاده از منابع را داشته باشد.

۳,۵,۳ واکنش به تخطی‌ها از خط‌مشی ترافیک شبکه

محصول باید با پیکره‌بندی مدیران IPS، قابلیت واکنش بلادرنگ برای خاتمه دادن یا مسدود کردن ترافیک‌هایی را که از خط‌مشی‌های تعریف شده توسط مدیر IPS تخطی می‌کنند را داشته باشد.

۳,۵,۴ مدیریت محصول

برای پوشش دادن تهدید مربوط به دسترسی مدیریتی غیرمجاز که در سند پروفایل حفاظتی مطرح شده است، انطباق محصولات امکان تعریف توابع ضروری را برای مدیران جهت پیکره‌بندی توانایی‌های IPS محصول، فراهم می‌سازند.

۳,۵,۵ ارتباطات مورد اطمینان

برای پوشش بهتر تهدیدات مربوط به ارتباطات غیرقابل اطمینان کانال‌ها که در سند پروفایل حفاظتی تعریف شده است، انطباق محصولات ارتباطات قابل اطمینان بین مؤلفه‌های توزیع شده، در صورت وجود، فراهم خواهد ساخت.

۳,۶ الزامات کارکرد امنیتی

این سند توسعه داده شده پروفایل حفاظتی تجهیزی شبکه و دیواره آتش است. الزامات کارکرد امنیتی IPS در جدول زیر ارائه و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول آمده‌اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن‌ها را رعایت نمایند. بر اساس انتخاب‌هایی که در این الزامات صورت می‌گیرند، لازم خواهد بود که برخی الزامات مورداشاره در پیوست دو نیز رعایت شوند. برخی الزامات اختیاری نیز ممکن است از پیوست یک برگزیده شوند. موارد ذکرشده در قالب فعالیت‌های ارزیابی، بیان می‌کنند که توسعه‌دهندگان محصول مورد ارزیابی باید چه مواردی را رعایت کنند.

جدول ۳-۱: لیست الزامات پروفایل

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	مدیریت کارکرد در محصول IPS۱	FMT_SMF.1.1
۴	کارکرد IPS مبتنی بر رفتار غیرعادی ۱	IPS_ABD_EXT.1.1
۵	کارکرد IPS مبتنی بر رفتار غیرعادی ۲	IPS_ABD_EXT.1.2
۶	کارکرد IPS مبتنی بر رفتار غیرعادی ۳	IPS_ABD_EXT.1.3
۷	بلوکه کردن آدرس IP ۱	IPS_IPB_EXT.1.1
۸	بلوکه کردن آدرس IP ۲	IPS_IPB_EXT.1.2
۹	تحلیل ترافیک شبکه ۱	IPS_NTA_EXT.1.1
۱۰	تحلیل ترافیک شبکه ۲	IPS_NTA_EXT.1.2
۱۱	تحلیل ترافیک شبکه ۳	IPS_NTA_EXT.1.3
۱۲	کارکرد IPS مبتنی بر امضاء ۱	IPS_SBD_EXT.1.1
۱۳	کارکرد IPS مبتنی بر امضاء ۲	IPS_SBD_EXT.1.2
۱۴	کارکرد IPS مبتنی بر امضاء ۳	IPS_SBD_EXT.1.3

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۵	کارکرد IPS مبتنی بر امضاء ۴	IPS_SBD_EXT.1.4
۱۶	کارکرد IPS مبتنی بر امضاء ۵	IPS_SBD_EXT.1.5
پیوست یک: الزامات اختیاری		
۱۷	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1
۱۸	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
۱۹	محل ذخیره‌سازی داده‌های ممیزی ۷	FAU_STG_EXT.4.1
۲۰	مدیریت رفتار توابع امنیتی IPS ۱	FMT_MOF.1.1
۲۱	مدیریت داده‌های محصول IPS ۱	FMT_MTD.1.1
۲۲	نقش امنیتی ۳	FMT_SMR.2.1
۲۳	نقش امنیتی ۴	FMT_SMR.2.2
۲۴	نقش امنیتی ۵	FMT_SMR.2.3
۲۵	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۲۶	انتقال داده‌های امنیتی در داخل محصول ۱	FPT_ITT.1.1
۲۷	تخصیص منابع ۱	FRU_RSA.1.1
۲۸	نرمال‌سازی ترافیک ۱	IPS_SBD_EXT.2.1
۲۹	نرمال‌سازی ترافیک ۲	IPS_SBD_EXT.2.2
۳۰	نرمال‌سازی ترافیک ۳	IPS_SBD_EXT.2.3

۳,۷ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که مدیر سیستم، اطلاعات لازم برای شناسایی مشکلات موجود درزمینهٔ پیکربندی و/یا کارکرد سیستم را در اختیار دارند، محصول باید امکان تولید داده‌های ممیزی موردنیاز را داشته باشد. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش‌شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این‌که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که محصول مورد ارزیابی یا راهبران مسئول بازبینی این اطلاعات را دچار سردرگمی کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت امن خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل‌اعتماد باشند. این امر سبب می‌شود که بتوان

اطلاعات را پس از ارسال به دستگاه‌های خارجی مرتب کرد. از دست رفتن ارتباط با سرور ممیزی می‌تواند مشکل‌ساز شود. هرچند که راه‌های مختلفی برای کاهش این تهدید وجود دارد، اما این پروفایل حفاظتی هیچ اقدام خاصی را الزام نمی‌کند. مناسب بودن محصول مورد ارزیابی در یک محیط خاص، متأثر از میزان حفاظت از اطلاعات ممیزی با این اقدامات و توانایی محصول مورد ارزیابی برای انجام کارکردهای خود در اثر انجام اقدامات مذکور است.

از محصول مورد ارزیابی دستگاه‌های شبکه انتظار نمی‌رود که تمام داده‌های ممیزی را ذخیره کند. هرچند که لازم است داده‌ها به‌صورت محلی در زمان تولید ذخیره شوند و در صورت تجاوز از ظرفیت ذخیره‌سازی، اقدامات مقتضی صورت گیرند، محصول مورد ارزیابی همچنین باید بتواند یک لینک امن را با یک سرور ممیزی خارجی ایجاد کند تا بتوان داده‌های ممیزی خارجی را ذخیره کرد.

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**
محصول باید بتوانند از رویدادهای قابل ممیزی IPS زیر، یک رکورد ممیزی تولید نمایند: الف) شروع و پایان توابع IPS ب) همه رویدادهای متفاوت IPS ج) همه واکنش‌های توابع IPS د) تعداد رویدادهای مشابه که در واحد زمان مشخص روی داده است ه) تعداد اقدامات متقابل که در واحد زمان مشخص روی داده است. **نکته کاربردی:** نویسنده سند هدف امنیتی برای لیست رویدادهای ممیزی در سند هدف امنیتی تنها به موارد ذکر شده در این الزام محدود نمی‌گردد و باید «جدول رویدادها» ذکر شده در الزام ۲ را با اطلاعات اضافه‌تر تکمیل کند. رویدادهای غیرمشابه آن دسته از رویدادهای هستند که به غیر از زمان از نظر سایر ویژگی‌های دیگر نیز متفاوت هستند. رویدادهای مشابه آن دسته از رویدادهای را شامل می‌شود که در یک بازه زمانی روی و دارای ویژگی مشابه هستند ولی تنها زمان آن‌ها متفاوت است.	
۲	**تولید داده ممیزی ۲**
محصول مورد ارزیابی باید در هر یک از رویدادهای ممیزی IPS، دست‌کم اطلاعات زیر را ثبت نماید: الف) تاریخ و زمان رویداد، نوع رویداد و واکنش رویداد ب) در مورد هر یک از انواع رویدادهای ممیزی IPS و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی، اطلاعات مشخص‌شده در نکته کاربردی زیر.	

نکته کاربردی:

همان‌طور که در نکته کاربردی قبل بیان شد، نویسنده سند هدف امنیتی باید جدول رویدادهای زیر با اطلاعات اضافه دیگری همچون آدرس‌های مبدأ و مقصد،IP، امضاء که رویداد بر اساس آن تریگر شده است، پورت، غیره تکمیل نماید.

نام الزام	رویدادهای ممیزی	اطلاعات اضافه رکوردهای ممیزی
مدیریت کارکرد محصول IPS ۱	تغییرات در المان‌های خط‌مشی‌های IPS	شناسه‌ها یا نام المان‌های خط و مشی‌های IPS تغییر یافته (به عنوان نمونه کدام امضاء، مبنا، لیست‌های سیاه و سفید تغییر داده شده است)
کارکرد IPS مبتنی بر رفتار غیرعادی	ترافیک بازرسی شده که با خط‌مشی IPS مبتنی بر رفتار غیرعادی انطباق دارد.	آدرس‌های IP مبدأ و مقصد
		محتوای فیلدهای سرآیند که با خط‌مشی‌های مشخص شده انطباق دارد.
		واسطی که از آن بسته دریافت شده است.
		جنبه‌هایی از خط‌مشی‌های قوانین مبتنی بر ناهنجاری که رویداد تریگر شده است (به عنوان نمونه گذردهی، زمان روز، فرکانس و ...).
		واکنش محصول در مقابل رویداد (اجازه داده شده است، مسدود شده است، هشدار مسدود شدن به فایروال ارسال شده است)
بلوکه کردن آدرس IP ۱	انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا	آدرس‌های IP مبدأ و مقصد (و در صورت امکان، نشانه‌ای دال بر این که این آدرس‌های مبدأ و/یا مقصد منطبق با لیست هستند یا خیر)
		واسط محصول که بسته را دریافت کرده است.
		اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستور reset)
تحلیل ترافیک شبکه ۱	تغییر این که کدام خط‌مشی‌های پیشگیری از نفوذ روی واسط محصول فعال هستند. فعال کردن و غیرفعال کردن واسط	شناسایی واسط محصول
		خط‌مشی پیشگیری از نفوذ و مد واسط (در صورت امکان)

	محصول که خط‌مشی‌های پیشگیری از نفوذ روی آن اعمال شده‌اند. تغییر این که کدام مُدها روی واسط محصول فعال هستند.	
کارکرد IPS مبتنی بر امضاء ۱	انطباق ترافیک بازرسی‌شده با خط‌مشی پیشگیری از نفوذ مبتنی بر امضا	نام یا شناسه امضای انطباق‌داده‌شده
		آدرس‌های IP مبدأ و مقصد.
		محتوای فیلدهای سرآیند که باید با خط‌مشی انطباق داشته باشند.
		محصول که بسته را دریافت کرده است.
		اقدامی که محصول در شبکه انجام می‌دهد (مانند اجازه دادن، مسدود کردن، ارسال دستور reset)
نرمال‌سازی ترافیک ۱ (اختیاری)	بازرسی بسته‌های کپسوله‌شده	شناسایی روش کپسوله‌سازی
نرمال‌سازی ترافیک ۲ (اختیاری)	شکست در سر هم کردن مجدد بسته‌های چندتکه‌ای[۱]	آدرس‌های IP مبدأ و مقصد
		واسط محصول که تکه‌ها[۲] را دریافت کرده است.
نرمال‌سازی ترافیک ۳(اختیاری)	نرمال‌سازی ترافیک توسط محصول	آدرس‌های IP مبدأ و مقصد بسته‌های کنار گذاشته‌شده[۳] واسط محصول که بسته‌ها را دریافت کرده است

۳,۸ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش مدیر سیستم و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (کارکرد مدیریتی محصول)، مدیریت داده‌های محصول مورد ارزیابی (مدیریت داده‌های محصول) و فعال کردن به‌روزرسانی‌های محصول مورد ارزیابی (مدیریت کارکرد در محصول ۱ (۱)/به‌روزرسانی‌های امن) هستند. در کنار این الزامات مدیریتی اصلی، برخی الزامات اختیاری نیز در پیوست اول و تعدادی الزامات انتخابی نیز در پیوست دوم ذکر شده‌اند.

[۱] Fragmented packets
[۲] Fragments
[۳] Discarded packets

شماره الزام	نام الزام
۳	**مدیریت کارکرد در محصول IPS۱**

محصول مورد ارزیابی باید قادر به انجام توابع مدیریتی زیر باشد:
]
۱) فعال‌سازی، غیر فعال‌سازی امضاهایی که در واسطهای حسگر به کار می‌روند و تعیین رفتار کارکرد IPS
۲) تغییر و اصلاح این پارامترهایی که جمع‌آوری و تحلیل ترافیک شبکه را تعیین می‌کنند:
الف) آدرس‌های IP مبدأ (آدرس میزبان و آدرس شبکه)
ب) آدرس‌های IP مقصد (آدرس میزبان و آدرس شبکه)
پ) پورت مبدأ (TCP و UDP)
ت) پورت مقصد (TCP و UDP)
ث) پروتکل (IPv4 و IPv6)
ج) کد و نوع ICMP
۳) به‌روزرسانی (وارد کردن) امضاها
۴) ایجاد امضاهای خاص
۵) پیکربندی کشف رفتارهای غیرعادی
۶) فعال‌سازی و غیر فعال‌سازی اقدامات هنگامی که امضا یا رفتارهای غیرعادی مورد شناسایی قرار می‌گیرند.
۷) تغییر آستانه‌هایی که واکنش‌های IPS را هدف می‌گیرند.
۸) تغییر مدت زمان بلوکه کردن ترافیک
۹) تغییر لیست سیاه و لیست سفید (از آدرس‌های IP و بازه آدرس‌ها)
۱۰) پیکربندی لیست سیاه و لیست سفید برای نادیده گرفتن خط‌مشی‌های IPS مبتنی بر امضا
[

۳,۹ کلاس IPS: جلوگیری از نفوذ

شماره الزام	نام الزام
۴	**کارکرد IPS مبتنی بر رفتار غیرعادی ۱**

محصول باید از تعریف [انتخاب: (انتخاب حداقل یکی یا هر دو): مبنا[۱] (مورد انتظار و تأییدشده)، الگوهای ترافیکی ناهنجار (غیر انتظار)] پشتیبانی کند و شامل مشخصات زیر باشد:

[انتخاب:

- توان عملیاتی[۲] ([الزام: عناصر داده‌ها (مثل بیت‌ها، بسته‌ها و غیره) در واحد زمان (مثل دقیقه، ساعت، روز و غیره)])
- زمان روز
- تناوب
- آستانه‌ها
- [اختصاص: روش‌های دیگر] و هیچ روش دیگر]

و فیلدهای پروتکل شبکه زیر:

[انتخاب: تمامی سرآیند بسته و عناصر داده‌ها که در «الزام کارکرد IPS مبتنی بر امضاء» تعریف شده‌اند؛ [الزام: لیست زیرمجموعه سرآیند بسته و عناصر داده‌ها از «الزام کارکرد IPS مبتنی بر امضاء»]]

نکته کاربردی:

مبناها، ترافیک خوب شناخته شده را تعریف می‌کنند (که در الزام «کارکرد IPS مبتنی بر رفتار غیرعادی ۳» مجاز شمرده شده است) در حالی که ترافیک ناهنجار، تعریف «ترافیک متخلف» است که باید با اقدامات دیگری که در الزام «کارکرد IPS مبتنی بر رفتار غیرعادی ۳» تعریف شده با آن مواجه شد.

تناوب را می‌توان چنین تعریف کرد: تعداد دفعات وقوع هر رویداد (مثل شناسایی بسته‌هایی که مطابق با یک امضا هستند) طی یک بازه مشخص زمانی، مانند تعداد نشست‌های FTP که طی یک ساعت ایجاد می‌شوند. اگر «تناوب‌ها» انتخاب شوند، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف تناوب‌ها در محصول ارائه کند.

آستانه‌ها را می‌توان این‌گونه تعریف کرد: میزان یا درصد انحراف از مرزها یا سطوح مورد انتظار، مثل تعداد مگابایت‌هایی که هر ساعت از FTP عبور می‌کنند. اگر «آستانه‌ها» انتخاب شود، «خلاصه مشخصات محصول» باید توضیحی از نحوه تعریف آستانه‌ها در محصول ارائه نماید.

۵	**کارکرد IPS مبتنی بر رفتار غیرعادی ۲**

محصول باید از تعریف فعالیت غیرعادی از طریق: [انتخاب: پیکربندی دستی توسط سرپرست، پیکربندی خودکار] پشتیبانی نماید.

نکته کاربردی:

[۱] Baselines

[۲] Throughput

مبنا و ناهنجاری گاهی می‌توانند به صورت دستی توسط سرپرست محصول، پیکربندی/تعیین شوند، یا چیزی که محصول بتواند آن را به صورت خودکار با بازرسی ترافیک شبکه طی بازه زمانی مشخص، تعریف/ایجاد کند (به این کار پروفایلینگ نیز گفته می‌شود). لازم نیست که محصول IPS قابلیت «پروفایلینگ» شبکه را داشته باشد تا مبنا یا قاعده‌ای را به صورت پویا تعریف کند و اگر محصول IPS این کارکرد را داشته باشد، چنین کارکردی به عنوان بخشی از بسته تکمیلی IPS مورد ارزیابی قرار نمی‌گیرد.

۶	**کارکرد IPS مبتنی بر رفتار غیرعادی ۳**

محصول باید به عملیات زیر اجازه دهد که با خط‌مشی‌های مبتنی بر رفتارهای غیرعادی ترکیب شوند.

- در هر حالتی، برای هر واسط حسگری: [انتخاب:
  - اجازه به جریان ترافیک
  - ارسال یک بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  - ارسال یک بازنشانی TCP به آدرس مقصد ترافیک متخلف
  - ارسال یک پیام غیرقابل دسترسی ICMP [انتخاب‌ها: میزبان، مقصد، پورت]
  - هدف‌گیری یک ابزار شبکه‌ای غیر محصول برای بلوکه کردن الگوی ترافیک متخلف]
- در حالت درون‌خطی:
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک

و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از محصول عبور کنند، بدون هیچ اقدام دیگر]

۷	**بلوکه کردن آدرس IP ۱**

محصول باید از پیکربندی و پیاده‌سازی لیست سیاه و لیست سفید از آدرس‌های IP [انتخاب: آدرس مبدأ، آدرس مقصد] پشتیبانی نماید.

نکته کاربردی:

نوع آدرس‌هایی که در این تابع هدف امنیتی تعریف شده است، محدود است به آدرس‌های IP (مثل یک آدرس IP واحد یا بازه‌ای از آدرس‌های IP) زیرا این بسته تکمیلی IPS، به بازرسی ترافیک IP محدود است. هدف‌های ارزیابی از نوع IPS از فعال‌سازی کارکردهایی که جریان ترافیک را بر اساس انواع دیگر آدرس (مثل MAC) متوقف/ مجاز کنند، جلوگیری نمی‌نماید؛ اما زمانی که از این کارکرد استفاده می‌شود، مستندات دستورالعمل‌ها و «خلاصه مشخصات محصول» باید شرح دهند که چه نوع پیکربندی باعث ایجاد لیست آدرس‌های سفید و سیاه غیر IP شده‌اند تا بر لیست آدرس‌های مبتنی بر IP اولویت یابد.

۸	**بلوکه کردن آدرس IP ۲**

محصول باید به سرپرست IPS و [انتخاب: هیچ نقش دیگر [الزام: نقش‌های دیگر]] اجازه دهد که عناصر خط‌مشی IPS را پیکربندی نماید (قوانین لیست سیاه، قوانین لیست سفید، آدرس‌های IP).	
۹	**تحلیل ترافیک شبکه ۱**
محصول باید ترافیک شبکه مبتنی بر IP را که به واسط‌های سنسور محصول جریان دارد، مورد تجزیه و تحلیل قرار دهد و نقض خط‌مشی‌هایی که توسط سرپرست تعریف شده را شناسایی نماید. **نکته کاربردی:** اگرچه ممکن است در برخی محصولات، هر واسط محصول بتواند به عنوان واسط سنسور عمل نماید، ولی این موارد مورد نظر نیستند. در این الزام اصطلاح «واسط سنسور» برای هر واسط محصول که یک یا چند خط‌مشی IPS روی آن اعمال شده است، استفاده می‌شود. یک خط‌مشی IPS سرپرستی تعریف‌شده، به هر مجموعه‌ای از قوانین برای تحلیل ترافیک، مسدودسازی ترافیک، تشخیص امضاء و/یا تشخیص ناهنجاری اعمال شده بر روی یک یا چند واسط سنسور، گفته می‌شود. ممکن است محصول بتواند به سرپرست اجازه دهد که اولویت المان‌های خط‌مشی امنیتی (لیست سیاه و سفید، قوانین مبتنی بر امضاء و قوانین مبتنی بر ناهنجاری) را پیکربندی نماید، ولی چنین پیکربندی‌هایی در این سند الزام نیستند.	
۱۰	**تحلیل ترافیک شبکه ۲**
محصول باید پروتکل‌های ترافیک شبکه زیر را پردازش کند (بتواند بازرسی کند): • پروتکل اینترنت (IPv4)، RFC 791 • پروتکل اینترنت نسخه ۶ (IPv6)، RFC 2460 • پروتکل پیام کنترل اینترنت نسخه ۴ (ICMPv4)، RFC 792 • پروتکل پیام کنترل اینترنت نسخه ۶ (ICMPv6)، RFC 2463 • پروتکل کنترل انتقال (TCP)، RFC 793 • پروتکل داده‌های کاربر (UDP)، RFC 768 **نکته کاربردی:** تطابق با پروتکل‌های RFC به منزله این نیست که محصول باید تضمین کند تمامی بسته‌ها در تمامی اوقات از پروتکل‌های RFC پیروی می‌کنند. همچنین به منزله این نیست که محصول می‌تواند در هر جریان ترافیکی در هر زمانی، به طور کامل از RFC پیروی کند. تطابق با پروتکل‌های RFC چارچوب مرجعی است برای فهم محتوای بسته‌ها (سرآیندها، فیلدها، وضعیت‌ها، فرمان‌ها و غیره) که در این الزام کارکرد امنیتی و دیگر الزامات، شناسایی شده‌اند؛ یعنی محصول باید بتواند پیاده‌سازی RFC را تا حدی بفهمد که پارامترهای RFC از طریق الزامات کارکرد امنیتی مشخص شود.	

۱۱	تحلیل ترافیک شبکه ۳

محصول باید برای واسط‌های حسگر پیکربندی شده در حالت‌های بی‌قاعده[۱] و درون‌خط امضاهایی را تخصیص دهد و از طراحی یک یا چند واسط به عنوان مدیریت ارتباطات بین محصول و موجودیت‌های خارجی پشتیبانی کند بدون این‌که به طور هم‌زمان واسط‌های حسگر باشند.

- حالت بی‌قاعده (فقط شنود): [الزام: فهرستی از انواع واسط]،
- حالت درون‌خط (داده‌های عبوری): [الزام: فهرستی از انواع واسط]،
- حالت مدیریت: [الزام: فهرستی از انواع واسط]،
- [انتخاب:
  - واسط‌هایی با قابلیت راه‌اندازی مجدد نشست: [الزام: فهرستی از انواع واسط]،
  - [الزام: انواع دیگر واسط‌ها [الزام: فهرستی از انواع واسط]]،
  - و هیچ نوع دیگری از انواع واسط] .

نکته کاربردی:

انواع واسط‌ها ممکن است اترنت، گیگابیت اترنت و غیره باشد. واسط‌های بی‌قاعده، واسط‌هایی هستند که ترافیک شبکه را به منظور بازرسی شبکه شنود می‌کنند، اما هیچ کارکردی در لایه‌های ۲،۳ و بالاتر فراهم نمی‌آورند؛ بنابراین سرویس‌های شبکه بر روی واسط‌ها شنود نمی‌شوند و هیچ پشته پروتکل IP بر روی واسط فعال نیست، در نتیجه هیچ آدرس IP به واسطی اختصاص داده نمی‌شود. واسط‌های درون‌خط، جفت واسط‌هایی هستند که مسیری را برای ترافیک شبکه فراهم می‌آورند به‌طوری‌که بتوان جریان شبکه را بلوکه و یا توسط محصول ویرایش کرد. واسط‌های بی‌قاعده و درون‌خط کارکردهای لایه ۳ و بالاتر را پشتیبانی نمی‌کنند، آن‌ها ممکن است کارکردهای لایه ۲ را فراهم نمایند (با آدرس فیزیکی نسبت داده شده به واسط‌ها) تا اجازه دهند دستگاه‌های شبکه، ترافیک شبکه را به محصول ارسال و یا دریافت کنند.

۱۲	کارکرد IPS مبتنی بر امضاء ۱

محصول باید از بازرسی محتوای سرآیند بسته‌ها پشتیبانی نماید و بتواند حداقل سرآیند فیلدهای زیر را بازرسی نماید:

- IPv4: نسخه، طول سرآیند، طول بسته، پرچم IP، ID، آفست تکه[۲]، زمان فعالیت (TTL)، پروتکل، سرآیند چک‌سام، آدرس مبدأ، آدرس مقصد، گزینه‌های IP و[انتخاب: نوع سرویس (ToS)، هیچ فیلد دیگری] .
- IPv6: نسخه، طول محتوا، سرآیند بعدی، محدودیت گام، آدرس مبدأ، آدرس مقصد، سرآیند مسیریاب و[

[۱] Promiscuous

[۲] Fragment

انتخاب: کلاس ترافیک، برچسب جریان، هیچ فیلد دیگری] .

- ICMP: نوع، کد، چک‌سام سرآیند و [انتخاب: ID، شماره توالی، [اختصاص: سایر فیلدها در سرآیند ICMP]]
- ICMPv6: نوع، کد و چک‌سام سرآیند
- TCP: پورت مبدأ، پورت مقصد، عدد توالی، عدد تصدیق، آفست، رزرو، پرچم‌های TCP، پنجره، چک‌سام، نشانگر اضطراری و گزینه‌های TCP
- UDP: پورت مبدأ، پورت مقصد، طول و چک‌سام UDP

۱۳	**کارکرد IPS مبتنی بر امضاء ۲**

محصول باید از بازرسی محتوای سرآیند بسته‌های پشتیبانی کند و قادر باشد حداقل فیلدهای سرآیند زیر را بازرسی کند تا فرایند تطابق الگوهای مبتنی بر رشته‌های داده را اجرا کند:

- داده‌های ICMPv4: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP
- داده‌های ICMPv6: کاراکترهایی بیشتر از ۴ بیت اول از سرآیند ICMP
- داده‌های TCP (کاراکترهایی بیشتر از ۲۰ بیت سرآیند TCP)، با پشتیبانی برای شناسایی:

- دستورات FTP (انتقال فایل): help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, type.
- دستورات و محتوای HTTP (وب): دستوراتی شامل GET و POST و رشته‌های تعیین‌شده توسط سرپرست مطابق با URL/URI ها و محتوای صفحه وب.
- وضعیت SMTP (ایمیل): شروع وضعیت، وضعیت دستورات SMTP، وضعیت سرآیند mail، وضعیت بدنه mail، وضعیت قطع فرایند.
- [انتخاب: [اختصاص: دیگر انواع بازرسی محتوای TCP]

- داده UDP: کاراکترهایی بیشتر از هشت بیت اول سرآیند UDP
- [اختصاص: دیگر انواع بازرسی محتوای بسته‌ها]

علاوه بر این، توابع امنیتی محصول باید از بازترکیب استریم پشتیبانی کند و قادر به شناسایی محتوای مخرب باشد، حتی اگر در چند بسته‌ی مختلف تقسیم شده باشد.

۱۴	**کارکرد IPS مبتنی بر امضاء ۳**

محصول باید قادر به کشف امضاهای مبتنی بر سرآیند (با استفاده از فیلدهای مشخص شده در IPS_SBD_EXT.1.1) در واسط‌های حسگر IPS باشد.

- حملات IP
  - هم‌پوشانی تکه‌های IP(حمله Teardrop، حمله Bonk و یا حمله Boink)

○ یکسان بودن آدرس IP مبدأ با آدرس IP مقصد - حملات ICMP ○ ترافیک تکه‌ای ICMP (برای مثال حمله Nuke) ○ ترافیک حجیم ICMP (حمله Ping of Death) - حملات TCP ○ TCP NULL flags ○ TCP SYN+FIN flags ○ TCP FIN only flags ○ TCP SYN+RST flags - حملات UDP ○ حمله UDP Bomb ○ حمله UDP Chargen DoS
۱۵ **کارکرد IPS مبتنی بر امضاء ۴**
توابع امنیتی محصول باید بتواند تمامی امضاهای کشف الگوی ترافیکی زیر را شناسایی کند و این امضاها را در واسط حسگر IPS به کار گیرد: • سیل‌آسا به میزبان (حمله DoS) ○ سیل‌آسا ICMP (حمله Smurf، سیل‌آسا ping) ○ سیل‌آسا TCP (مثل سیل‌آسا SYN) • سیل‌آسا به شبکه (حمله DoS) • اسکن پورت و پروتکل (حملات شناسایی که آدرس‌های IP را برای یافتن سرویس‌های باز/ فعال/ در حال شنیدن اسکن می‌کنند.) ○ اسکن پروتکل IP ○ اسکن پورت TCP ○ اسکن پورت UDP ○ اسکن ICMP **نکته کاربردی:** این الزام حداقل مجموعه از فیلدهای بسته سرآیند، رشته‌های بسته بار، انواع امضاء و الگوهای ترافیک بدخواه بالقوه (مانند: سیل‌آسا و پویش) که محصول باید تشخیص دهد را، تعریف می‌نماید. امضاهای معتبر ممکن است با یک، برخی و یا همه مشخصه‌های بیان شده در این الزام تطابق یابد و همچنین محصولات IPS ممکن است مشخصه های بیشتری نسبت به آنچه لیست شده است را جهت بررسی، پشتیبانی نمایند ولی فقط موارد لیست شده در این الزام باید توسط ارزیاب‌ها مورد آزمون قرار گیرند. مجموعه مشخصه‌های، انواع امضاها، الگوهای ترافیک و غیره؛ که

در الزام ذکر شده است، به منظور شناسایی کامل فعالیت‌های بدخواهانه یا حملات DDoS نیست. هدف از این الزام پوشش حملاتی است که از یک آدرس IP صورت می‌گیرد. پویش پورت و پروتکل، به شناسایی حملاتی که با هدف قرار دادن چندین پورت/پروتکل بر روی یک یا چند آدرس IP، هدف را برای سرویس‌های باز/پاسخگو و ... پویش می‌کند، اشاره دارد.

۱۶	**کارکرد IPS مبتنی بر امضاء ۵**

محصول به عملیات زیر اجازه می‌دهد تا با خط‌مشی‌های IPS مبتنی بر امضا، ترکیب شوند:

- در هر حالتی، برای هر واسط حسگر: [انتخاب:
  - اجازه به جریان ترافیک
  - ارسال بازنشانی TCP به آدرس مبدأ ترافیک متخلف
  - ارسال بازنشانی TCP به آدرس مقصد ترافیک متخلف
  - ارسال پیام غیرقابل دسترسی ICMP انتخاب: میزبان، مقصد، پورت
  - هدف‌گیری یک ابزار شبکه‌ای غیر محصول برای بلوکه کردن الگوی ترافیک متخلف]
- حالت بر خط
  - اجازه به جریان ترافیک
  - بلوکه کردن/ قطع جریان ترافیک
  - و [انتخاب: اصلاح و ارسال بسته‌ها قبل از اینکه از محصول عبور کنند، بدون هیچ اقدام دیگری]

۴ پیوست یک

در این بخش الزامات اختیاری بیان شده است و نویسنده سند هدف امنیتی می‌تواند با توجه به محصول زیرمجموعه‌ای از این الزامات را در سند هدف امنیتی بیان کند.

۴,۱ ممیزی امنیت

شماره الزام	نام الزام
۱۷	**محل ذخیره‌سازی داده‌های ممیزی ۱**
محصول باید داده‌های IPS ذخیره شده را از حذف غیرمجاز محافظت نماید.	
۱۸	**محل ذخیره‌سازی داده‌های ممیزی ۲**

شماره الزام	نام الزام
محصول باید قادر به [جلوگیری] از تغییرات غیرمجاز در داده‌های IPS ذخیره شده، باشد. **نکته کاربردی:** رویدادهای قابل‌ممیزی IPS اضافه‌ای که نیاز باشد در «تولید داده ممیزی» در نظر گرفته شود، وجود ندارد.	
۱۹	**محل ذخیره‌سازی داده‌های ممیزی ۷**
محصول در صورت پر شدن داده IPS، باید [انتخاب: «رویدادهای تولید شده توسط IPS را نادیده بگیرد»، «جلوگیری از ذخیره رویدادهای IPS»، «بر روی قدیمی‌ترین داده‌های IPS ذخیره شده دوباره‌نویسی نماید».]	

۴,۲ الزامات مدیریت امنیت

شماره الزام	نام الزام
۲۰	**مدیریت رفتار توابع امنیتی IPS ۱**
محصول باید توانایی [تغییر رفتار] توابع [جمع‌آوری داده IPS، آنالیز کردن، واکنش] را به [سرپرست مجاز IPS] محدود نماید.	
۲۱	**مدیریت داده‌های محصول IPS ۱**
محصول باید قادر به محدود کردن [انتخاب: تغییر پیش‌فرض، پرس‌وجو، ویرایش، حذف، پاک کردن، [اختصاص: عملیات دیگر]] و [اختصاص: فهرستی از داده‌های IPS] به [اختصاص: سرپرست IPS، تحلیل‌گر IPS و دیگر نقش‌های مشخص‌شده در الزام «نقش امنیتی ۳»] باشد. **نکته کاربردی:** نویسنده سند هدف امنیتی باید نقش‌هایی که اجازه دسترسی به داده‌های IPS را دارند، مشخص کند (سرپرست IPS، تحلیل‌گر IPS و دیگر نقش‌های مشخص شده در الزام «نقش امنیتی ۳»). نویسنده سند هدف امنیتی ممکن است تنها تعدادی از نقش‌های مورد نیاز را معین کند	
۲۲	**نقش امنیتی ۳**
محصول، باید **نقش‌های زیر** را نگهداری نمایند: • سرپرست IPS، • تحلیل‌گر IPS • [انتخاب: [اختصاص: دیگر نقش‌های IPS مجاز]، هیچ نقش دیگری]	

شماره الزام	نام الزام
۲۳	**نقش امنیتی ۴**
محصول باید قادر به مرتبط کردن کاربران با نقش‌هایشان باشد.	
۲۴	**نقش امنیتی ۵**
محصول باید اطمینان دهد که [اختصاص: شرایط برای نقش‌های متفاوت] برآورده می‌شود.	

۴,۳ الزامات محافظت از هدف ارزیابی

شماره الزام	نام الزام
۲۵	**حفظ وضعیت امن در زمان شکست ۱**
محصول قادر است وضعیت امن را برای واسط‌های درون‌خط وقتی که انواع شکست زیر روی می‌دهد حفظ کند: [اختصاص: لیست از انواع شکست توابع محصول]	
۲۶	**انتقال داده‌های امنیتی در داخل محصول ۱**
محصول باید از [افشاء شدن یا تغییر] داده توابع خود زمانی که بین [اختصاص: فهرستی از بخش‌های مجزای محصول] منتقل می‌گردد با استفاده از [انتخاب: با یک یا بیش از یکی از پروتکل‌های:IPSEC،SSH،TLS،HTTPS] محافظت نماید. **نکته کاربردی:** بر اساس انتخابی که در این الزام صورت می‌گیرد، الزامات مربوط به هر کدام از انتخاب‌های صورت گرفته شده باید بر اساس تعریف آن الزام در پروفایل حفاظتی پایه، در سند هدف ارزیابی آورده شوند.	

۴,۴ الزامات تخصیص منابع

شماره الزام	نام الزام
۲۷	**تخصیص منابع ۱**
محصول باید حداکثر سهمیه را برای منابع تخصیص دهد: [اختصاص: منابعی که از نظارت بر روی ترافیک شبکه پشتیبانی کنند] که [موجودیت‌های فعال] می‌توانند هم‌زمان استفاده کنند.	

شماره الزام	نام الزام
نکته کاربردی: هدف این الزام حصول اطمینان از این است که محصول طوری توسعه داده نشده باشد که جریان داده روی واسط‌های سنسور از مقداری که محصول می‌تواند بررسی نماید، سرریز کند. اگر جریان (حجم/سرعت) داده که باید مورد بررسی قرار گیرد، از سهم تعیین شده سرریز کند، محصول باید یک اخطار در رابطه با این سرریز تولید نماید.	

۴,۵ الزامات IPS: جلوگیری از نفوذ

در این بخش الزاماتی با توجه به پیاده‌سازی عملیات نرمال‌سازی بسته‌های شبکه در IPS می‌تواند به سند هدف امنیتی اضافه شود.

شماره الزام	نام الزام
۲۸	**نرمال‌سازی ترافیک ۱**
محصول باید قادر به نظارت بر بسته‌های محصور شده از طریق [انتخاب:GRE، IP-in-IP،IPv4-in-IPv6،MPLS،PPTP، [اختصاص: دیگر روش‌های محصورسازی]، هیچ روش دیگر] باشد.	
۲۹	**نرمال‌سازی ترافیک ۲**
محصول باید قادر به نرمال‌سازی برای بازترکیب بسته‌های تکه‌تکه شده برای نظارت و [انتخاب: • برای داده جمع شده در واسط‌های promiscuous: در صورتی که نتوان بازترکیب را انجام داد، تولید یک پیام هشدار. • برای داده جمع شده در واسط‌های درون‌خط: بسته‌های تکه‌تکه شده را هدایت نکرده و یک هشدار تولید کرده که نمی‌توان بسته موجود را بازترکیب کند.]	
۳۰	**نرمال‌سازی ترافیک ۳**
محصول باید نرمال‌سازی TCP را برای جریان‌های ترافیک از طریق محصول در حالتی که محصول در مد درون‌خط مستقر شده داشته باشد و از هدایت [انتخاب: بسته‌های تکراری، بسته‌های تغییر داده شده، بسته‌های خارج از توالی،[انتخاب: [اختصاص: دیگر انواع بسته‌ای که نباید ارسال گردد]، هیچ بسته دیگری]] جلوگیری کند.	

۵ پیوست دو: تعاریف

۵,۱ تعریف حملات

نام	توضیحات
DoS	حمله DoS (Denial of Service)
Flooding	جاری ساختن سیل عظیمی از ترافیک روی یک زیرشبکه IP یا علیه یک آدرس IP خاص
IP Impossible Packet (Land)	بسته‌های IP که آدرس مبدأ و مقصد آن‌ها یکسان است (Land Attack)
IP options Bad Option List	دیتاگرام IP که لیست گزینه‌های IP در سرآیند آن ناقص یا دستکاری‌شده هستند.
IP options Record Packet Route	دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۷ می‌شود (Record Packet Route)
IP options Timestamp	دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۴ می‌شود (Timestamp)
IP options Security	دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۲ می‌شود (Security)
IP options Loose Source Route	دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۳ می‌شود (Loose Source Route)
IP options Strict Source Route	دیتاگرام IP که لیست گزینه‌های IP آن شامل گزینه ۲ می‌شود (Strict Source Route)
IP Overlapping Fragments (Teardrop, Bonk)	دو تکه داده موجود در یک دیتاگرام IP واحد دارای آفست‌هایی دال بر موقعیت مشترک آن‌ها در دیتاگرام هستند. این امر می‌تواند بدین معنی باشد که تکه الف به طور کامل یا ناقص توسط تکه ب بازنویسی شده است.
ICMP fragments (Ping of Death, Nuke)	فیلد پروتکل سربرگ IP دیتاگرام IP روی ۱ تنظیم می‌شود (ICMP)، بیت تکه آخر[1] تنظیم می‌گردد و (آفست IP * ۸) + (طول داده IP) باید بزرگ‌تر از ۶۵۵۳۵ باشد. آفست ارائه دهنده موقعیت ابتدایی این تکه در بسته اولیه است و در واحدهای ۸ بایتی قرار دارد) به علاوه بقیه بسته، بزرگ‌تر از حداکثر اندازه یک بسته IP است.

[1] Last Fragment bit

نام	توضیحات
ICMP flooding (Smurf, ping flood)	آدرس IP مقصد در بسته عبارت است از آدرس پخش[۱] زیرشبکه مقصد، به گونه‌ای که تمام ماشین‌های روی این زیرشبکه به پخش پاسخ دهند.
Scanning (IP protocols, TCP ports, UDP ports)	تلاش برای تعیین این که آیا خدمات گوش دادن روی برخی شماره‌های پروتکل IP، پورت‌های TCP یا پورت‌های UDP خاص موجود هستند یا خیر. برای این کار، مجموعه‌ای از داده‌ها ارسال می‌شوند تا یک پاسخ مورد انتظار تولید گردد.
TCP FIN only flags	بسته‌های TCP FIN بی‌هویت[۲]، به یک پورت دارای دسترسی ویژه فرستاده می‌شوند (شماره پورت‌های پایین‌تر از ۱۰۲۴)
TCP flood (SYN flood)	ارسال تعداد بسیار زیادی بسته TCP با پرچم SYN تنظیم‌شده به منظور فزونی گرفتن از محدودیت تعداد نشست‌های TCP نیمه‌باز.
TCP NULL flags	یک بسته TCP که هیچ‌یک از پرچم‌های SYN، FIN، ACK یا RST آن تنظیم نشده است به یک میزبان خاص فرستاده می‌شود.
TCP SYN+FIN flags	بسته TCP که پرچم‌های SYN و FIN آن تنظیم شده است.
UDP Bomb attack	طول UDP تعیین‌شده کمتر از طول IP تعیین‌شده است. این نوع بسته تغییرشکل‌یافته با یک حمله DoS همراه می‌شود.
UDP Chargen DoS attack	بسته UDP دارای پورت مبدأ ۷ و پورت مقصد ۱۹ است.

۵,۲ تعریف عبارات و مخفف‌ها

نام	توضیحات
ناهنجاری / ناهنجار (در مورد ترافیک شبکه)	ترافیکی که در دسته ترافیک‌های عادی تعریف‌شده نمی‌گنجد و بنابراین، غیرمنتظره و غیر نوعی است. ترافیک ناهنجار الزاماً خطرناک نیست و ضرورتاً شبکه پایش‌شده را تهدید نمی‌کند.

[۱] Broadcast

[۲] Orphaned TCP FIN packet

نام	توضیحات
ترافیک عادی[۱] (در مورد ترافیک شبکه)	تعریف می‌کند که کدام ترافیک‌های شبکه پایش‌شده، مورد انتظار یا عادی هستند. تمام ترافیک‌های عادی (ترافیک مبنا) الزاماً امن نیستند و عادی بودن ترافیک به این معنی نیست که تهدیدی برای شبکه پایش‌شده به شمار نمی‌آید. به عنوان مثال، ترافیک عادی می‌تواند با لیست آدرس‌های IP بد انطباق داشته باشد یا مطابق با امضای تهدیدات شناخته‌شده باشد.
مُد جریان درون‌خط	به‌کارگیری محصول (یا مؤلفه‌های آن) به گونه‌ای که ترافیک شبکه پایش‌شده الزاماً از محصول بگذرد و بدین ترتیب، محصول امکان مسدود کردن آن را داشته باشد.
IPS	سیستم پیشگیری از نفوذ[۲]
خط‌مشی IPS (خط‌مشی پیشگیری از نفوذ)	تمام مجموعه قوانینی که برای تحلیل ترافیک، مسدود کردن ترافیک، تشخیص امضا و/یا تشخیص ناهنجاری استفاده می‌شوند. بسیاری از خط‌مشی‌های IPS را می‌توان تعریف و روی محصول ذخیره کرد؛ اما این خط‌مشی‌ها بدون پیاده‌سازی (فعال‌سازی) روی یک یا چند واسط IPS اثری نخواهند داشت.
نرمال‌سازی (در مورد ترافیک شبکه)	فیلتر کردن ترافیک شبکه به گونه‌ای که تنها بسته‌ها یا تکه‌های مفید اجازه رسیدن به مقصد را داشته باشند. نرمال‌سازی تنها در صورتی توسط محصول قابل انجام است که محصول در مد جریان درونی به کار گرفته شده باشد. در فرایند نرمال‌سازی ممکن است بسته‌های تکراری، تکه‌هایی که نمی‌توان سر هم کرد، بسته‌های نامعتبر و بسته‌های دارای خارج از توالی، کنار گذاشته و فیلتر شوند.
پروفایلینگ (در مورد ترافیک شبکه)	مانند تعریف ترافیک عادی.

[۱] Baseline

[۲] Intrusion Prevention System

نام	توضیحات
مُد بی‌قاعده	حالتی از یک واسط IP که در آن واسط مذکور به ترافیک شبکه گوش می‌دهد (آن‌ها را جمع‌آوری و بازرسی می‌کند). ممکن است منظور از یک واسط بی‌قاعده، واسطی باشد که فقط به ترافیک گوش می‌دهد و هرگز آن را منتشر نمی‌کند، یا واسطی که مثلاً در مد جریان درونی قرار دارد و جریان ورودی و خروجی ترافیک در آن برقرار است.
واسط حسگر	هر واسط محصول که خط‌مشی IPS در آن پیاده‌سازی شده است.